Fort Gordon Local Blackberry Users Training

a. All users will be held responsible for damage caused to a Government system or data through negligence or a willful act.

b. Users are not authorized and will not use Bluetooth technology with Blackberry devices except for the authorized CAC sled found on the Department of Defense (DOD) Unified Capabilities (UC) Approved Products List (APL) and the blueARMOR Bluetooth Wireless Headset approved by CIO/G-6.

c. No users will operate a wireless device in areas where classified information is electronically stored or processed.

d. All users will ensure the Blackberry handheld device is cradled or synced at least once every 30 days to the Blackberry Enterprise Server (BES) to receive updated keys and/or software updates.

e. All users must understand that all charges incurred in excess of the normal monthly service charge will be the responsibility of the Blackberry user. Excessive charges include: exceeding allocated minutes per month, downloading any applications, services, ringtones, games, etc., and neglect or abusive damage to the device or accessory.

f. All users will complete Portable Electronic Devices/Removable Media training at http://iase.disa.mil/eta/pedrm_v2/pedrm_v2/index.htm.

(Right click on the link to start the training and select open hyperlink)

Fort Gordon Local Blackberry Users Training (Cont)

g. All users will be aware of the following risks when utilizing the SMS service:

(1) Messages are not encrypted and copies are not stored in memory on the phone or in the wireless carrier database. Sensitive information should not be sent via SMS/Text/Messages/Multimedia Messaging Service (MMS).

(2) URL to hacker websites can be sent to a SMS/Text Message/MMS. If a user connects to the URL, malware could be downloaded on the phone.

(3) Executable files (including malware) can be embedded in SMS/Text Message/MMS.

Fort Gordon Local Blackberry Users Training (Cont)

(4) Photos sent via SMS/Text Messages/MMS can have URLs to hacker websites embedded in the photo. When the photo is viewed, the phone will connect to website of the embedded website.

(5) Photos sent via SMS/Text Messages/MMS can have executable files (including malware) embedded in the photo. When a photo is viewed, the phone will execute the file.

Together, we can do great things…let's stay connected!